UN Bankcard Processing PCI Policy

POLICY CONTENTS

Scope

This policy applies to all systems and university employees that are subjected to and must adhere to the Payment Card Industry Data Security Standards (PCI-DSS).

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

Security Policies

Security policies covering university handling of bankcards will be established, published, maintained, and disseminated by each campus PCI DSS task force. The security policies will be reviewed at least annually, and when the PCI DSS requirements change.

This policy is in addition to existing acceptable use policies and proper technology usage policies covered in NU Executive Memorandums 16 and 26.

Responsibilities

There will be a PCI DSS task force team assigned on each university campus. The task force should include member(s) of the university Bursar's office or equivalent, as well as the university information security office.

Members of Information Technology Services will be responsible for managing the network cardholder data environment, including servers redirecting to a third party for the processing of bank cards. Distributed IT staff or ITS staff will be responsible for distributed point of sale systems.

Physical card swipe devices will be ordered and assigned by the Bursar's office or equivalent, per the university merchant application procedures.

Vulnerability scans will be performed by ITS staff and mitigated by the designated system administrator(s).

ITS staff will be responsible for creating, maintaining, and de-provisioning accounts and two-factor authentication to CDE systems as necessary.

The Bursar's office or equivalent office will maintain and implement policies and procedures to manage service providers.

Merchant departments will maintain written detailed internal procedures describing the proper handling of bankcard transactions for every payment channel they support.

Reason for Policy

This policy is to establish good internal controls over the handling of bankcard transactions to adequately safeguard and properly record university bank card assets and to protect the employees who handle those assets. Further, it is the policy of the university to comply with all state and federal regulations, Board of Regent policy and the Payment Card Industry Data Security Standards (PCI/DSS).

Definitions

Bankcard: defined as credit cards, debit cards, ATM cards and any other card or device, other than cash or checks, issued by a bank or credit union that is normally presented by a person seeking to make payment. The process of paying is considered as the transaction.

Cardholder Data: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Payment Card Industry Data Security Standards (PCI/DSS): guidance for organizations to assist in providing data security on payment card transactions.

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26

This policy covers the following sections of PCI-DSS 3.2:

- 12.1 Establish, publish, maintain, and disseminate a security policy
- 12.3 Develop usage policies for critical technologies and define proper use of technologies
- 12.4 Clearly define information security responsibilities for all personnel
- 12.5 Assign to an individual or team information security management responsibilities
- 12.8 Maintain and implement procedures to manage service providers

History

This policy is a new policy created in 2017.